L'USO "OBLIQUO" DEI DATI ESTERNI DELLE COMUNICAZIONI TRA ESPANSIONE DELLE GARANZIE SOVRANAZIONALI, INERZIA DEL LEGISLATORE E INCERTEZZE INTERPRETATIVE

di Luigi Parodi
(*Dottorando di ricerca in* Security and Law*, Università di Genova*)

1. Il tema della conservazione e dell'acquisizione dei dati sul traffico telefonico e telematico rappresenta, come noto, uno dei terreni sui quali si registrano tensioni tra esigenze di tutela della sicurezza e di garanzia dei diritti fondamentali degli individui[1].

[1] Come si vedrà, i diritti fondamentali che vengono in rilievo sono, in particolare, quello alla tutela della vita privata e familiare, alla protezione dei dati personali e alla libertà e segretezza delle comunicazioni. Il tema del bilanciamento di tali diritti con le esigenze di sicurezza e accertamento è di fondamentale rilevanza, anche e soprattutto nell'ambito dell'elaborazione dottrinale e giurisprudenziale sul rapporto tra nuove tecnologie e processo penale. Sul valore della *privacy* nella materia di cui si tratta, cfr., in particolare, L. Lupária, *Privacy, diritti della persona e processo penale*, in *RDP* 2019, 1449, il quale afferma che tale diritto fondamentale rappresenta oggi «il baluardo in grado di proteggere l'individuo contro l'avanzata incontrollata di alcune forme «aggressive» di intelligenza artificiale, in grado di travolgere i pilastri di garanzia in vari campi del diritto, tra cui anche la procedura penale»; M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano 2021, 56 ss. Sui termini del bilanciamento in discorso, cfr. M. Daniele, *La prova digitale nel processo penale*, in *RDP* 2011, 287 ss.; C. Conti, *Sicurezza e riservatezza*, in *DPP* 2019, 1572 ss.; G. De Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normativa*, in *Rivista AIC*, 4/2019, 79 ss.; F. Centorame, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *RIDPP* 2021, 499 ss.; con più specifico riferimento al tema della *data retention*, G. Formici, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino 2021, *passim*, spec. 19 ss., 341

L'attenzione degli interpreti, finora, si è concentrata prevalentemente sulle questioni connesse all'uso "primario" dei dati nel procedimento penale. In tale prospettiva, gli sforzi esegetici della dottrina e l'evoluzione giurisprudenziale – dovuta soprattutto alle numerose pronunce della Corte di giustizia dell'Unione europea – in materia di *data retention* hanno consentito la progressiva emersione di un quadro di principi, in parte recepiti dal legislatore interno, volti a tutelare le prerogative individuali dalle potenzialità intrusive dello strumento investigativo di cui si tratta[2].

Rispetto al fulcro del dibattito così avviato un aspetto di significativa rilevanza è tuttavia rimasto a lungo in un cono d'ombra. Si tratta del tema dell'uso "obliquo" (o "secondario") dei dati raccolti e utilizzati conformemente al diritto dell'Unione, per tale intendendosi il trasferimento degli stessi, per qualsivoglia esigenza di accertamento, dal procedimento di prima acquisizione a una diversa regiudicanda. A tal proposito, si pone il delicato problema di accertare se, ed eventualmente a quali condizioni, il descritto uso "obliquo" sia consentito in relazione alle informazioni legittimamente acquisite, in origine, in determinati procedimenti penali per finalità di contrasto alle forme gravi di criminalità.

La questione problematica appena evocata riguarda sia la circolazione probatoria in materia penale, sia il trasferimento dei dati in procedimenti *extra*-penali: la ricostruzione della disciplina applicabile, in entrambi i casi richiamati, non è agevole. Le fonti europee, che notoriamente rivestono fondamentale rilevanza in questa materia, non regolano infatti espressamente l'uso "obliquo" dei dati. Lo stesso si può affermare, peraltro, anche con riguardo alla disciplina interna: l'art. 132 d.lgs. 30.6.2003 n. 196 (d'ora in avanti, cod. *privacy*) disciplina soltanto la conservazione e la prima acquisizione dei tabulati nel procedimento penale.

La ricerca delle coordinate normative per l'uso "obliquo" dei dati esteriori delle comunicazioni costituisce dunque operazione complessa, rispetto alla quale è ineludibile il confronto con la portata dei diritti fondamentali rilevanti in tema di *data retention*.

In quest'ottica, nei paragrafi successivi, si analizzeranno anzitutto le indicazioni provenienti dalla giurisprudenza europea, pronunciatasi di recente anche sul tema di cui si tratta. Successivamente, si rivolgerà lo sguardo all'ordinamento interno, esaminando l'indirizzo pretorio che ha finora consentito il libero trasferimento dei

ss.; A. Malacarne, G. Tessitore, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di Giustizia: ancora inadeguata la disciplina interna?*, in *www.archiviopenale.it,* 3/2022, 3 ss.

[2] Il tema verrà trattato nel prosieguo: v., in particolare, par. 2.

tabulati all'esterno e all'interno dei procedimenti penali e interrogandosi sulla sua legittimità alla luce dei principi fondamentali di ordine costituzionale e sovranazionale. Riguardo alla seconda ipotesi menzionata, l'indagine si concentrerà soprattutto sulla ricerca di possibili soluzioni – compatibili con i richiamati principi – in materia di circolazione probatoria delle informazioni, sia in chiave interpretativa, sia in un'ottica *de iure condendo*.

2. La riflessione sul tema appena tratteggiato richiede di soffermarsi *in primis* sul contributo, consistente e articolato, offerto dalla Corte di giustizia dell'Unione europea.

Nell'ambito del controverso processo di regolamentazione della materia di cui si tratta, i *dicta* della Corte di giustizia – come noto – hanno svolto un ruolo essenziale, anche e soprattutto nella prospettiva della tutela dei diritti fondamentali degli individui, posti a rischio dall'impiego di misure connotate da una spiccata attitudine intrusiva. La giurisprudenza della Corte, infatti, ha contribuito a delineare un vero e proprio statuto giuridico della *data retention*, interpretando l'unica fonte unionale oggi vigente in materia – la direttiva 2002/58/CE – alla luce dei pertinenti principi della Carta dei Diritti Fondamentali dell'Unione europea (di seguito anche semplicemente Carta)[3]. Tale percorso ermeneutico ha condotto la Corte, per il tramite di numerose pronunce di carattere indubbiamente innovativo, a ricavare una disciplina sempre più articolata del fenomeno[4].

La giurisprudenza della Corte di giustizia in materia si era finora sviluppata in diversi passaggi.

Il primo è costituito dalla storica sentenza *Digital Rights Ireland,* con la quale la Corte di giustizia ha dichiarato l'invalidità della direttiva 2006/24/CE (in materia di *data retention*) per contrasto con i diritti sanciti dagli articoli 7 e 8 CDFUE, letti alla

[3] In questo senso L. Lupária, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Dir. di internet* 2019, 757 ss.; F.R. Dinacci, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *PPG* 2022, 310 ss.; S. Marcolini, *La giurisprudenza della Corte di giustizia dell'Unione europea sulla* data retention*; il baluardo dei diritti fondamentali in Europa*, in R. Flor, S. Marcolini, *Dalla* data retention *alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Torino 2022, 11 ss.; L. Filippi, *Riservatezza e* data retention: *una storia infinita*, in *www.penaledp.it,* 23.6.2022;

[4] Sul punto cfr., ad esempio, P. Di Stefano, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?*, in *CP* 2022, 2564, il quale ritiene che la Corte di giustizia, a partire dalla sentenza *Digital Rights Ireland*, abbia proceduto a "disciplinare" il fenomeno della *data retention* attraverso un'interpretazione della direttiva in funzione significativamente integrativa del suo disposto.

luce del principio di proporzionalità, di cui al successivo art. 52, par. 1, della medesima Carta[5]. Molteplici le ragioni della ravvisata incompatibilità: il carattere generalizzato della *retention*; il riferimento ai reati definiti "gravi", secondo una formula troppo generica; la mancata previsione di un controllo sull'accesso ai dati da parte di un'autorità indipendente; i termini molto prolungati entro i quali era possibile conservare le informazioni[6].

Il successivo passaggio si deve alle sentenze *Ministerio Fiscal*[7] e *La Quadrature du Net*[8], le quali hanno individuato in modo più puntuale i criteri da applicare nella verifica della proporzionalità delle misure che consentono l'accesso alle informazioni sul traffico, prendendo in considerazione fattori quali il grado di ingerenza nei diritti fondamentali e la gravità dei fenomeni criminosi da contrastare. Occorre sottolineare che tale indirizzo è stato arricchito da due recenti pronunce, con le quali la Corte ha ulteriormente precisato la portata e i confini di siffatta valutazione. In particolare, da un lato, si sono specificati i presupposti – dal punto di vista delle modalità tecniche di conservazione e dei criteri per l'utilizzazione delle informazioni – alla stregua dei quali l'accesso ai dati sull'identità civile degli utenti relativi a indirizzi IP già conservati in modo generalizzato non costituisce un'ingerenza grave nelle prerogative fondamentali degli individui[9]. Dall'altro si è affermata la necessità di consentire al giudice di negare l'accesso ai dati quando il reato per il quale si procede, pur in astratto appartenente alla categoria della criminalità grave, vi risulti manifestamente estraneo in concreto[10].

Il terzo *step* è stato compiuto con la nota sentenza sul caso *Prokuratuur*, ove si è chiarito che l'autorità preposta a disporre l'accesso ai dati non può essere il pubblico

[5] Il riferimento è a C.G.UE, Grande Sezione, *Digital Rights Ireland Ltd*, 8.4.2014, C-293/12 e C-594/12, ECLI:EU:C:2014:238, sulla quale v.: R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d.* «data retention» *contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in *DPenCont*, 2/2014, 178 ss.; L. Trucco, Data retention: *la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *GI* 2014, 1850 ss.; F. Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harvard Human Rights Journal* 2015, 65 ss.; S. Marcolini, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in *Cybercrime,* diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano 2019, 1582 ss.; G. Formici, *La disciplina della* data retention, cit., 68 ss.

[6] Sul tema, cfr. S. Marcolini, *La giurisprudenza della Corte di giustizia*, cit., 10 s.

[7] C.G.UE, *Ministerio Fiscal*, Grande Sezione, 2.10.2018, C-207/16, ECLI:EU:C:2018:788.

[8] C.G.UE, Grande Sezione, *La Quadrature du Net* e a., 6.10.2020, C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791.

[9] C.G.UE, Grande Sezione, *La Quadrature du Net*, C-470/21, 30.4.2024, ECLI:EU:C:2024:370.

[10] C.G.UE, Grande Sezione, 30.4.2024, C-178/22, ECLI:EU:C:2024:371, sulla quale v. D. Albanese, *Dalla Corte di giustizia dell'Unione europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*, in *www.sistemapenale.it*, 14.5.2024.

ministero, in ragione del suo ruolo di parte processuale[11].

Infine, altre importanti decisioni hanno esaminato le diverse – e meno invasive – forme di investigazione tecnologica che possono essere impiegate dalle autorità nazionali degli Stati membri in alternativa o in aggiunta alla *data retention*, nella prospettiva del contenimento della lesione delle prerogative fondamentali degli individui[12].

Con una recente sentenza[13], la Corte di giustizia ha poi aggiunto un'ulteriore tessera al mosaico delineato in materia di *data retention*, trattando per la prima volta il tema dell'uso "obliquo" dei dati sul traffico. I giudici europei hanno, infatti, avuto occasione di chiarire che il diritto dell'Unione osta all'utilizzo dei dati personali relativi alle comunicazioni elettroniche, raccolti e acquisiti in un procedimento penale per finalità di lotta alla criminalità grave, nell'ambito di procedimenti diversi che non perseguano obiettivi di pari o superiore importanza.

I principi affermati in tale decisione – che si inserisce, in modo armonico, nella descritta traiettoria evolutiva – hanno una diretta incidenza sulle questioni trattate nel presente lavoro. Sembra quindi opportuno ripercorrere la vicenda presa in esame dalla Corte e l'*iter* argomentativo seguito per giungere alla soluzione dei quesiti interpretativi ad essa devoluti.

3. La Corte di giustizia si è pronunciata a seguito di un rinvio pregiudiziale promosso dalla Corte Amministrativa Suprema lituana, avente ad oggetto l'interpretazione dell'art. 15 della direttiva 2002/58/CE[14].

[11] Cfr. C.G.UE, *H.K* (*Prokuratuur*), Grande Sezione, 2.3.2021, C-746/18, ECLI:EU:C:2021:152; cfr. n. 30 per gli opportuni riferimenti bibliografici.

[12] Il riferimento è, in particolare, alla sentenza *Commissioner of An Garda Síochána* e a., 5.4.2022, C-140/20, ECLI:EU:C:2022:258, con la quale la Corte ha ribadito il divieto di una *retention* generalizzata e indifferenziata, chiarendo però che, per finalità di contrasto alla criminalità grave e di prevenzione di minacce alla pubblica sicurezza, gli Stati possono legittimamente prevedere diverse misure, per certi versi meno intrusive, segnatamente: la conservazione generalizzata dei dati relativi all'identità civile degli utenti e, per un periodo limitato allo stretto necessario, degli indirizzi IP; la conservazione "mirata" dei dati, delimitata sulla base di criteri oggettivi e non discriminatori; l'ingiunzione rivolta ai *provider* di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e all'ubicazione dei *device* ("*quick freeze*").

[13] C.G.UE, Sez. I, *A.G.*, 7.9.2023, C-162/22, ECLI:EU:C:2023:631, sulla quale v. i commenti di Di Stefano, *La Corte di giustizia ribadisce che i dati di traffico telefonico e telematico regolarmente conservati ed acquisiti al fine di lotta alla criminalità grave, di tutela della sicurezza pubblica e della sicurezza dello stato non possono essere ulteriormente utilizzati per finalità diverse. Vietato ogni uso dei tabulati al di fuori del processo penale?*, in *CP* 2023, 4285 ss.; F. Resta, *L'uso "secondario" dei tabulati nell'interpretazione della CGUE*, in *www.giustiziainsieme.it*, 20.9.2023.

[14] Come noto, tale disposizione consente agli Stati membri di derogare al divieto generale di memorizzazione

La Procura Generale aveva avviato un'indagine disciplinare nei confronti del ricorrente, all'epoca dei fatti procuratore, sospettato di aver illegittimamente fornito all'indagato e al suo difensore informazioni rilevanti riguardo a un'indagine da lui diretta. Ai fini dell'accertamento dell'illecito venivano utilizzati i dati relativi alle telecomunicazioni raccolti, conformemente alla disciplina nazionale in materia, in sede penale[15], i quali contribuivano in maniera decisiva al riconoscimento della responsabilità disciplinare[16].

Le doglianze relative all'illegittima lesione dei diritti fondamentali del ricorrente richiamavano l'attenzione della Corte di ultima istanza, inducendola a sollevare la questione pregiudiziale. Il giudice del rinvio domandava, nello specifico, «[s]e l'articolo 15, paragrafo 1, della direttiva 2002/58, in combinato disposto con gli articoli 7, 8, 11 e 52, paragrafo 1, della Carta, debba essere interpretato nel senso che esso vieti alle autorità pubbliche competenti di utilizzare, nell'ambito di indagini per condotta illecita di natura corruttiva nell'esercizio di funzioni pubbliche, i dati conservati dai fornitori di servizi di comunicazione elettronica che possono fornire informazioni sui dati di un utente di un mezzo di comunicazione elettronica e sulle comunicazioni da questi effettuate, indipendentemente dal fatto che l'accesso a tali dati sia stato concesso, nel caso concreto, ai fini del contrasto di reati gravi e di prevenzione di gravi minacce alla sicurezza pubblica».

Era in questione, in particolare, se le condizioni di cui all'art. 15 della direttiva 2002/58, interpretato alla luce della Carta, dovessero essere rispettate anche con riferimento all'uso successivo dei dati sul traffico, conservati e messi a disposizione dell'autorità per finalità di contrasto alla criminalità grave o di prevenzione di gravi minacce alla sicurezza pubblica. Nello specifico, occorreva stabilire se anche l'uso "secondario" di tali dati costituisse un'ingerenza nei diritti fondamentali sanciti, anzitutto, dagli articoli 7 e 8 della Carta, di gravità tale da poter essere giustificata solo

dei dati posto dal precedente art. 5, «qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica».

[15] Oggetto della domanda erano, in particolare, i dati conservati in forza dell'articolo 65, paragrafo 2, della legge lituana sulle comunicazioni elettroniche, che impone ai *provider* l'obbligo di conservare, in modo generalizzato e indifferenziato, i dati relativi al traffico e quelli relativi all'ubicazione, ai fini della lotta alla criminalità grave.

[16] Come rilevato dal giudice adito per l'impugnazione delle sanzioni irrogate, i dati erano stati acquisiti conformemente alle disposizioni della disciplina interna. Secondo la legge lituana sull'*intelligence* criminale, infatti, le informazioni provenienti da indagini penali relative a un fatto di natura corruttiva possono essere "declassificate", con il consenso del pubblico ministero, e utilizzate nell'ambito di un'indagine disciplinare

dal perseguimento degli obiettivi desumibili dall'art. 15.

Come prevedibile, per rispondere al quesito, i giudici europei compiono un imprescindibile riferimento ad alcuni dei principi affermati dai propri precedenti in materia di *data retention*.

Anzitutto, la Corte mette in luce il fondamentale punto di partenza del proprio percorso argomentativo: l'utilizzo dei dati è consentito solo a condizione che la conservazione e il successivo accesso ai medesimi si siano svolti in conformità con l'art. 15 della direttiva, come interpretato dalla giurisprudenza europea[17]. A tal proposito, si ribadisce che una *retention* generalizzata e indiscriminata dei dati relativi al traffico e all'ubicazione, quale strumento di contrasto alla criminalità grave e di prevenzione di gravi minacce alla pubblica sicurezza, si pone in aperto contrasto con il diritto dell'Unione[18].

La statuizione appena riportata trova fondamento e giustificazione alla luce del principio di proporzionalità che, come noto, costituisce il *leitmotiv* dell'elaborazione della Corte di giustizia (anche) in materia di *data retention*[19]. Il tema è, dunque, quello del delicato bilanciamento tra la garanzia dei diritti fondamentali degli individui – nella specie, il diritto al rispetto della vita privata e familiare e alla protezione dei dati – e le esigenze di accertamento dei reati e di salvaguardia della sicurezza pubblica[20]. Proprio in tale prospettiva, la Corte ha individuato una serie di criteri sulla base dei quali condurre il vaglio di proporzionalità delle misure legislative che dispongono la *retention*.

Da un lato, occorre prendere atto dell'esistenza di diversi livelli di ingerenza. Infatti, non tutti i dati sono uguali: secondo l'insegnamento della Corte di giustizia, quella conservazione generalizzata che è vietata con riferimento ai dati relativi al traffico e all'ubicazione è invece consentita con riguardo agli indirizzi IP e ai dati che rivelano la

[17] A tal proposito, la Corte richiama il proprio precedente, pronunciato dalla Grande Sezione, nel procedimento penale a carico di *H.K* (*Prokuratuur*), cit., § 29; nello stesso senso si veda anche C.G.UE, Grande Sezione, *La Quadrature du Net e a.*, cit.

[18] Il richiamo è, in particolare, alla sentenza C.G.UE, Grande Sezione, *SpaceNet* e *Telekom Deutschland*, 20.9.2022, C-793/19 e C-794/19, ECLI:EU:C:2022:702, § 74 e 131. Peraltro, tale principio era già stato affermato in diverse altre sentenze della Corte di Giustizia, quali, segnatamente, *Digital Rights Ireland*, cit., § 56 ss.; C.G.UE, Grande Sezione, *Tele2*, 21.12.2016, C-203/15 e C-698/15, ECLI:EU:C:2016:970, § 107; *La Quadrature du Net* e a., cit.; *Commissioner of An Garda Síochána* e a., cit., § 65.

[19] La bibliografia in materia è amplissima. Per l'inquadramento del principio in materia processuale penale v., per tutti, M. Caianiello, *Il principio di proporzionalità nel procedimento penale*, in *DPenCont*, 3-4/2014, 143 ss.; con specifico riferimento al settore delle investigazioni tecnologiche, v., per tutti, F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria*, Milano 2020, 107 ss.

[20] Sul tema si rinvia, per gli opportuni riferimenti bibliografici, *supra*, alla n. 1.

sola identità anagrafica degli utenti[21]. Il metro di giudizio è l'attitudine dei dati a rivelare informazioni precise sulla vita privata degli individui ai quali si riferiscono[22]. La conservazione dei dati dotati di piena potenzialità "rivelatrice" è pertanto legittima *(i)* solo quando accuratamente delimitata alla stregua di criteri – elaborati in modo da non risultare discriminatori – di carattere soggettivo o geografico e *(ii)* a condizione che sia prevista per il periodo di tempo strettamente necessario al perseguimento dello scopo[23].

Dall'altro lato, neppure tra gli obiettivi che legittimano la conservazione dei dati vi è identità di rilevanza. Come ribadito nella sentenza sul caso *A.G.*, esiste una gerarchia tra i medesimi, dalla quale dipende il livello di ingerenza tollerabile nel perseguirli[24]. Secondo l'indirizzo accolto dalla Corte, al vertice della scala gerarchica si posiziona la salvaguardia della sicurezza nazionale. Seguono, poi, la prevenzione delle minacce gravi alla sicurezza nazionale e la lotta contro la criminalità grave[25]. Intercorre pertanto, ad avviso della Corte, una stretta correlazione tra l'importanza dell'obiettivo pubblicistico perseguito e la legittimità di un determinato grado di compressione dei diritti fondamentali in conseguenza della misura adottata, proprio in ossequio al principio di proporzionalità.

A ulteriore, coerente definizione del quadro appena tratteggiato si afferma, infine, che l'accesso ai dati può essere consentito solo per perseguire il medesimo obiettivo posto alla base della conservazione, oppure uno più importante[26].

In base alle premesse così delineate, si perviene a fornire la soluzione al quesito

[21] Così, ad esempio, la sentenza *SpaceNet*, cit., § 75. Cfr., in proposito, A. Malacarne, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi princìpi in materia di* data retention, in *RIDPP* 2021, 1165, il quale sottolinea come la natura non "grave" dell'ingerenza derivante da misure che non consentano di ricostruire le condizioni di vita degli utenti, nella prospettiva delineata dalla Corte di Giustizia con le sentenze *Ministerio Fiscal* e *La Quadrature du Net*, le renda applicabili con riferimento a qualunque fattispecie di reato. Come si è già accennato, la Corte è di recente tornata sul tema con la sentenza C.G.UE, Grande Sezione, *La Quadrature du Net*, C-470/21, 30.4.2024, cit.

[22] Sul tema si rinvia a *infra*, par. 6.4.

[23] Ancora, *SpaceNet*, cit., *loc. ult. cit.* Già a partire dal *leading case Digital Rights Ireland*, cit., § 59, nel ritenere incompatibile con il diritto dell'Unione una conservazione generalizzata e indiscriminata dei dati, la Corte aveva indicato – quali possibili soluzioni per delimitare l'ambito della conservazione – il criterio geografico e quello soggettivo, oltre a quello temporale.

[24] In questo senso, la pronuncia *Commissioner*, cit., § 56.

[25] Nella sentenza, al § 38, si sottolinea che l'obiettivo della lotta contro la criminalità grave può superare, a sua volta, quelli della lotta alla criminalità in generale e della prevenzione di minacce non gravi alla sicurezza pubblica.

[26] Il principio era già stato affermato dalla Corte nelle sentenze *La Quadrature du net*, cit., § 166 e *Commissioner*, cit., § 98.

sollevato. Ad avviso della Corte, i principi richiamati debbono applicarsi, *mutatis mutandis*, all'uso successivo dei dati relativi al traffico e all'ubicazione conservati a norma dell'art. 15 della direttiva. In particolare, i dati messi a disposizione dell'autorità per finalità di lotta alla criminalità grave non possono essere trasmessi ad altre autorità per il perseguimento di finalità diverse e di minore rilievo nella gerarchia degli obiettivi di interesse generale tracciata dalla giurisprudenza europea. Tale è considerato il caso di specie, in cui l'utilizzo dei dati era finalizzato all'accertamento in sede disciplinare di una condotta illecita di natura corruttiva.

Se è vero che la soluzione scaturisce dai principi già enunciati nei ben noti precedenti della Corte in materia di *data retention*, si deve tuttavia riconoscere l'apporto innovativo delle conclusioni da ultimo raggiunte nella sentenza in questione. La decisione ha avuto infatti il merito di chiarire che i diritti fondamentali in gioco possono subire una illegittima compressione non solo in occasione della conservazione dei dati sul traffico e della loro messa a disposizione delle autorità, ma anche a ogni successivo uso in altri procedimenti. Di conseguenza, gli stessi principi che guidano l'uso, per così dire, "primario" dei dati debbono essere rispettati quando venga in considerazione un uso "secondario". Primo fra tutti è quindi il limite della proporzione: l'uso dei dati, pur se in possesso di altre autorità e non più del *provider*, è consentito solo in relazione a un obiettivo di importanza tale da legittimare il corrispondente livello di ingerenza.

Opinare diversamente significherebbe tentare di aggirare le garanzie poste dal diritto dell'Unione, come interpretato dalla Corte, limitandone l'applicazione al primo utilizzo dei dati. Del resto, come già affermato dalla giurisprudenza di Lussemburgo, non sono consentite letture tali da giustificare che l'ingerenza nei diritti fondamentali degli individui, eccezionalmente consentita a determinate condizioni e per specifiche finalità, divenga la regola[27].

È il caso di sottolineare come dal principio enunciato dalla Corte di giustizia nella sentenza di cui si tratta paia emergere, *a contrario*, che il diritto dell'Unione non osti

[27] Nella sentenza *Tele2*, cit., § 89, la Corte ha chiarito che «l'articolo 15, paragrafo 1, della direttiva 2002/58, consentendo agli Stati membri di limitare la portata dell'obbligo di principio di garantire la riservatezza delle comunicazioni e dei dati relativi al traffico a queste correlati, deve essere interpretato, conformemente alla consolidata giurisprudenza della Corte, in maniera restrittiva (v., per analogia, sentenza del 22 novembre 2012, Probst, C-119/12, EU:C:2012:748, punto 23). Pertanto, una disposizione siffatta non può giustificare che la deroga al suddetto obbligo di principio e, in particolare, al divieto di memorizzare tali dati, previsto dall'articolo 5 della medesima direttiva, divenga la regola, a pena di privare quest'ultima norma di gran parte della sua portata». Il principio è stato ribadito più volte in successive pronunce.

all'uso "secondario" dei dati laddove questo avvenga nell'ambito di procedimenti che perseguono scopi di pari o superiore importanza rispetto a quelli che ne giustificano la conservazione. Non sarebbe dunque di per sé vietato il trasferimento dei dati da un procedimento ad un altro: tale ulteriore compressione delle prerogative di cui all'art. 8 della Carta sembrerebbe consentita a condizione che vengano rispettati i termini del bilanciamento che legittima la conservazione e l'accesso alle informazioni. Ciò pare valere, come si preciserà meglio nel prosieguo, a patto che la circolazione delle informazioni di cui si tratta sia adeguatamente disciplinata e corredata delle dovute garanzie sul piano dell'ordinamento interno.

4. Il tema affrontato ancora di recente dalla Corte di giustizia, in linea di coerente sviluppo dei propri precedenti in materia di *data retention*, riveste interesse e rilievo decisivi anche nella prospettiva dell'ordinamento italiano. Infatti, la giurisprudenza interna ha finora ammesso che i dati sul traffico, una volta acquisiti nel procedimento penale a norma dell'art. 132 d.lgs. 196/2003 (di seguito, cod. *privacy*), possano "circolare" liberamente ed essere utilizzati in altri procedimenti, penali ed *extra*-penali[28].

Appare scontato come tale quadro non possa rimanere immutato a fronte del richiamato contributo della Corte di giustizia, con il quale è stata precisata la portata dei principi sovranazionali con riferimento alle ipotesi di uso "secondario" dei dati. È ormai principio consolidato che le statuizioni interpretative della medesima sono vincolanti per l'interprete, in quanto chiariscono come una norma di diritto dell'Unione «deve, o avrebbe dovuto, essere intesa ed applicata dal momento della sua entrata in vigore»[29]. Anche la Corte costituzionale riconosce da tempo il carattere vincolante delle sentenze interpretative del Giudice europeo nei confronti del giudice nazionale, il quale ad esse deve attenersi nell'applicazione della disposizione oggetto della pronuncia[30].

[28] Sul tema, cfr. P. Di Stefano, *La Corte di giustizia*, cit., 4296 ss. Quanto ai procedimenti penali, v. Cass. 22.11.2007 n. 43329, in *OneLegale*; quanto a quelli *extra*-penali, ad esempio, Cass. Civ. 16.12.2020 n. 28757; Cass. Civ. 31.8.2020 n. 18096, ancora in *OneLegale*.

[29] Così, per tutte, C.G.UE, *Denkavit*, 27.3.1980, C-61/1979, § 16. Sul tema v. G. Leo, *Le indagini sulle comunicazioni*, cit., 16; A. Malacarne, *Corte di giustizia e* data retention, cit., 4123. Il medesimo principio è riaffermato, tra le altre, dalla sentenza *Commissioner*, cit., § 125, proprio con riferimento all'interpretazione della direttiva 2002/58.

[30] Lo sottolinea F.R. Dinacci, *L'acquisizione dei tabulati telefonici*, cit., 311 s.; il riferimento è, ad esempio, a C. cost., 21.6.2010 n. 227, in *www.cortecostituzionale.it*, nella quale si afferma che «le sentenze della Corte di giustizia vincolano il giudice nazionale all'interpretazione da essa fornita, sia in sede di rinvio pregiudiziale, che in sede di procedura d'infrazione». Il principio era già stato affermato tempo addietro, v. in particolare C. cost.,

Quanto agli effetti diretti della disciplina europea sulla *data retention* nell'ordinamento interno, non v'è invece identità di vedute[31]. Il tema si era posto con particolare urgenza in relazione alla sentenza *Prokuratuur*, alla luce della quale era emersa una radicale incompatibilità tra la disciplina interna sulla *data retention* e la rilevante normativa di diritto dell'Unione [32]. La consapevolezza dell'impatto "dirompente"[33] di tale pronuncia nell'ordinamento processuale italiano aveva costretto il legislatore a correre ai ripari, intervenendo sull'art. 132 cod. *privacy* per tentare di adeguarlo ai *dicta* della Corte. Prima di tale correttivo i giudici per le indagini preliminari, in qualche occasione, hanno disapplicato l'art. 132, riconoscendo effetto

4.7.1989 n. 389 e C. cost., 23.6.2005 n. 268, in *www.cortecostituzionale.it*. Nella sentenza citata da ultimo si afferma che «i princìpi enunciati dalla Corte di giustizia, riguardo a norme oggetto di giudizio di legittimità costituzionale, si inseriscono direttamente nell'ordinamento interno con il valore di *jus superveniens*, condizionando e determinando i limiti in cui quelle norme conservano efficacia e devono essere applicate anche da parte del giudice *a quo*». Peraltro, quando la Corte ritiene che la statuizione interpretativa non debba spiegare effetti *ex tunc*, in ragione di esigenze di certezza del diritto, provvede essa stessa a modulare nel tempo l'efficacia della decisione, come affermato già a partire dalla sentenza *Defrenne c. Sabena*, 8.4.1976, C-43/75. Tali principi sono affermati anche nella sentenza *La Quadrature du Net*, cit., § 216 e *Commissioner*, cit., § 119. *Amplius*, in argomento, A. Correra, *Natura ed effetti delle sentenze pregiudiziali della Corte di giustizia*, Napoli 2023, 172 ss.; E. Cimiotta, *L'ambito soggettivo di efficacia delle sentenze pregiudiziali della Corte di giustizia dell'Unione europea*, Torino 2023, 283 ss., il quale modula in termini problematici il vincolo *erga omnes* di conformità alle sentenze pregiudiziali della Corte.

[31] Una parte degli interpreti riconosce effetto diretto a tale disciplina: per F.R. Dinacci, *L'acquisizione dei tabulati telefonici*, cit., 311, la disapplicazione delle disposizioni interne contrastanti con la disciplina europea è una soluzione inevitabile, a fronte dell'immediata precettività dei principi enunciati dalla Corte di giustizia in materia di tabulati; nello stesso senso R. Flor, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali*, cit., 178; anche S. Marcolini, *La giurisprudenza della Corte di giustizia*, cit., 32 ss. propende decisamente per la necessità di disapplicare l'art. 132 cod. *privacy*, valorizzando soprattutto il contrasto con gli artt. 7 e 8 della Carta. Altra parte della dottrina, non ritenendo la disciplina sovranazionale dotata di effetto diretto, indica la via della prospettazione in via incidentale di una questione di legittimità costituzionale: così, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 193.

[32] Sul tema si rinvia ai numerosi commenti alla sentenza: cfr., per tutti, L. Filippi, *La disciplina italiana dei tabulati telefonici e telematici contrasta con il diritto U.E.*, in *www.dirittodidifesa.eu*, 20.3.2021; J. Della Torre, *L'acquisizione dei tabulati telefonici nel processo penale dopo la Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *www.sistemapenale.it*, 29.4.2021; G. Spangher, *I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, in www.*giustiziainsieme*.it, 3.3.2021; E. Andolina, *Ancora una pronuncia della Grande Camera della Corte di Giustizia UE in tema di condizioni di accesso ai* traffic data, in *PPG* 2021, 1195 ss.; G. De Amicis, *La Corte di giustizia si pronuncia sull'acquisizione dei tabulati telefonici e sull'accesso ai dati delle comunicazioni elettroniche nel processo penale*, in *CP* 2021, 2556 ss.; P. Di Stefano, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico*, cit.; A. Malacarne, *Corte di giustizia e* data retention: *ultimo atto?*, in *CP* 2021, 4104 ss. Il problema parrebbe porsi nuovamente, con una certa urgenza, in relazione alla già citata sentenza C.G.UE, Grande Sezione, 30.4.2024, C-178/22, che, pur non avendo censurato la scelta operata dal legislatore in merito all'individuazione della categoria di reati per i quali è consentito l'accesso ai dati, ha sottolineato la necessità di un vaglio di proporzionalità in concreto del giudice, allo stato non contemplato dall'art. 132 cod. *privacy*.

[33] L'espressione è di J. Della Torre, *L'acquisizione dei tabulati telefonici*, cit.

diretto alla disciplina europea in discorso, come interpretata dal Giudice di Lussemburgo[34]. Qualora si escludesse invece tale effetto, l'incompatibilità della disciplina interna con quella dell'Unione dovrebbe condurre alla sollevazione di una questione di legittimità costituzionale per violazione degli artt. 11 e 117 co. 1 Cost.[35].

Qualunque sia l'esito del dibattito, le letture che hanno finora consentito la "trasmigrazione" dei tabulati verso altri procedimenti devono ritenersi bandite, alla luce di quanto chiarito dalla recente pronuncia europea, laddove violino la gerarchia di interessi indicata dalla Corte.

Peraltro, sul punto è necessario operare una distinzione. Sembra infatti che le ricadute applicative dei principi posti alla base della decisione siano differenti a seconda che si vogliano utilizzare i dati sul traffico, acquisiti per finalità di accertamento di reati, in un procedimento penale ovvero in un giudizio *extra*-penale.

5. La prima ipotesi che deve essere esaminata è quella dell'uso "obliquo" dei dati al di fuori di un procedimento penale.

Non è un mistero che, fino a oggi, l'utilizzo dei tabulati raccolti in sede penale ai fini dell'accertamento *extra*-penale fosse una prassi consolidata: tale trasmigrazione avveniva tradizionalmente nell'ambito del processo civile (in materia giuslavoristica) e civile-tributario, del processo amministrativo in materia di impugnazione di sanzioni disciplinari e di quello dinanzi alla sezione disciplinare del Consiglio Superiore della Magistratura[36].

---

[34] Cfr. T. Roma, G.i.p., 25.4.2021, est. Sabatini, in *www.sistemapenale.it*, con nota di J. Della Torre, in cui si applica analogicamente la disciplina sulle intercettazioni; T. Bari, G.i.p., 1.5.2021, est. Agnino.

[35] La Corte costituzionale ha da tempo chiarito le diverse conseguenze a seconda che la disposizione interpretata abbia effetti diretti, oppure ne sia priva. Nella già citata sent. n. 227/2010 si ribadisce «il potere-dovere del giudice comune, e prima ancora dell'amministrazione, di dare immediata applicazione alle norme comunitarie provviste di effetto diretto in luogo di norme nazionali che siano con esse in contrasto insanabile in via interpretativa; ovvero di sollevare questione di legittimità costituzionale per violazione di quel parametro costituzionale quando il contrasto fosse con norme comunitarie prive di effetto diretto (sentenze n. 284 del 2007 e n. 170 del 1984)». Conforme, da ultimo, C. cost., 8.11.2022 n. 263, in *www.cortecostituzionale.it*. Tale impostazione va ora riconsiderata, in caso di doppia pregiudizialità determinata dalla contestuale contrarietà al parametro costituzionale e a disposizioni della CDFUE, alla luce della sentenza 7.11.2017 n. 269 della Corte costituzionale e delle successive pronunce che ne hanno precisato la portata, sia con riguardo alla priorità del giudizio costituzionale rispetto al rinvio pregiudiziale, sia con riferimento ai casi nei quali una disciplina interna appaia contraria a Costituzione e a disposizioni della Carta dotate di effetto diretto.

[36] Così, ad esempio, in Cass. Civ. 16.12.2020 n. 28757, cit.; Cass. Civ. 31.8.2020 n. 18096, cit. Si rinvia, sul punto, alla disamina svolta da P. Di Stefano, *La Corte di giustizia*, cit., 4295 ss., il quale ritiene tale linea interpretativa «del tutto conforme alla normativa in vigore sino al 2021», seppure da rivedere (e superare) a seguito della recente sentenza della Corte di Giustizia in tema di circolazione dei dati. Pienamente legittima rimarrebbe invece, secondo l'A., la valorizzazione della sentenza penale definitiva fondata sui dati di traffico.

Sembra opportuno interrogarsi sulla legittimità di simili letture, che sembrano difficilmente conciliabili con le esigenze di protezione dei diritti fondamentali che si pongono in materia di utilizzo dei dati sul traffico.

Una risposta al quesito che ci si pone pare rintracciabile direttamente nei principi affermati dalla Corte di giustizia nella sua pronuncia del 2023, più volte richiamata, sul caso *A.G.*, relativa proprio ad un'ipotesi di trasmigrazione dei dati all'esterno del procedimento penale.

È infatti possibile, alla stregua dei criteri enunciati in tale decisione, condurre un vaglio di compatibilità con il diritto dell'Unione delle letture che ammettono il trasferimento dei tabulati dal procedimento penale a quello *extra*-penale. In particolare, occorre verificare se l'obiettivo perseguito nell'ambito di tale giudizio rientri tra quelli che, secondo la giurisprudenza europea, legittimano la conservazione e l'accesso ai dati.

Ciò in quanto l'utilizzo dei dati esterni, comportando una rilevante compressione dei diritti tutelati dalla Carta, è consentito dall'ordinamento europeo in via del tutto eccezionale quando vengono in rilievo determinate esigenze di rilevanza pubblicistica. Come accennato sopra, il sistema sarebbe aggirato se le condizioni che legittimano l'uso dei dati rilevassero solo con riferimento alla prima acquisizione e, successivamente, i medesimi potessero circolare liberamente verso altre sedi procedimentali senza alcuna valutazione in ordine agli obiettivi perseguiti.

Una verifica nei termini appena descritti non sembra poter dare esito positivo. Pare possibile escludere, infatti, che con riguardo a tali procedimenti possano venire in rilievo le eccezionali istanze di accertamento e pubblica sicurezza descritte dalla giurisprudenza di Lussemburgo quali requisiti indispensabili per ammettere la circolazione. La considerazione trova un significativo riscontro nella sentenza sul caso *A.G.*, che ha riguardo ad una vicenda – pur tecnicamente non penalistica – strettamente connessa alla commissione di fatti di corruzione di rilevante gravità.

La Corte, malgrado il riconoscimento della rilevanza delle indagini disciplinari sugli illeciti di natura corruttiva nell'ambito della lotta contro tali fenomeni criminali, ha tuttavia negato la legittimità del trasferimento dei dati, osservando che simili procedimenti non rispondono «in modo effettivo e rigoroso all'obiettivo del perseguimento e della sanzione dei reati, di cui all'articolo 15, paragrafo 1» della direttiva[37]. Pare dubbio, poi, che procedimenti *extra*-penali possano attenere alla sfera

[37] In questi termini, C.G.UE, Sez. I, *A.G.*, 7.9.2023, C-162/22, *cit.*, § 43.

della salvaguardia della sicurezza pubblica, come dev'essere intesa ai fini della richiamata direttiva[38].

Se neppure un procedimento disciplinare volto all'accertamento di fatti corruttivi attribuiti a un magistrato soddisfa, quanto alla rilevanza degli obiettivi perseguiti, i requisiti posti dalla giurisprudenza europea, sembra possibile escludere, *a fortiori*, che altri procedimenti amministrativi o giudizi civili possano superare il medesimo vaglio.

6. Una volta esclusa la legittimità dell'utilizzo "obliquo" dei dati di traffico a fini *extra*-penali, sembra lecito domandarsi se e a quali condizioni i medesimi possano essere utilizzati in procedimenti penali diversi da quello principale.

Al riguardo, è utile ricordare che la Corte di giustizia non ha decretato la radicale incompatibilità con le fonti europee dell'uso dei dati in procedimenti diversi da quello principale. Tale utilizzo parrebbe ammissibile ove finalizzato al perseguimento di uno degli obiettivi che ne giustificano la conservazione e l'acquisizione.

Laddove si ritenessero legittime e giuridicamente fondate le prassi che hanno finora ammesso la trasmigrazione dei dati sul traffico, una soluzione coerente potrebbe essere quella, già prospettata in dottrina, di operare un'interpretazione orientata al diritto dell'Unione dell'art. 132 cod. *privacy*, tale da ritenere che l'uso dei dati in altri procedimenti sia consentito solo in relazione a reati che rientrano tra quelli indicati al terzo comma della stessa disposizione[39]. La riportata opzione ermeneutica garantirebbe il rispetto della gerarchia di obiettivi indicata dalla Corte di giustizia, limitando la possibilità di uso "secondario" dei dati all'ambito dei procedimenti per reati riconducibili alla categoria della "criminalità grave", quanto meno secondo l'accezione accolta dal legislatore interno[40].

[38] La questione era stata sollevata dai governi ceco e islandese. La Corte si è limitata ad osservare, sul punto, che il giudice del rinvio non aveva fatto menzione di minacce gravi alla sicurezza pubblica. Cfr., ancora, C.G.UE, Sez. I, *A.G.*, 7.9.2023, C-162/22, cit., § 42.

[39] In questo senso, P. Di Stefano, *La Corte di giustizia*, cit., 4297 ss. Un simile approccio sembra trovare riscontro negli *obiter dicta* di alcune recenti decisioni della Cassazione, ove si afferma che «[l]a Corte di giustizia ha, del resto, statuito che, una volta che la prova è stata acquisita nello spazio comune Europeo e in conformità al diritto dell'Unione, la sua ulteriore circolazione, con trasferimento ad altro procedimento, non richiede una nuova autorizzazione del giudice, ma solo che sia rispettato il limite della utilizzabilità per sicurezza pubblica e repressione di gravi reati». Così Cass. 7.12.2023 n. 48838; nello stesso senso Cass. 17.11.2023 n. 46482; Cass. 5.4.2024 n. 13819; Cass. 15.4.2024 n. 15417, tutte in *OneLegale*. È peraltro il caso di anticipare che, in materia di uso "obliquo" dei dati, il problema più delicato pare essere quello dell'individuazione di una disciplina che regoli e garantisca il trasferimento delle informazioni, nei casi in cui esso non sia vietato dal diritto dell'Unione.

[40] Sono stati sollevati dubbi sul rispetto, da parte del legislatore interno, del criterio della lotta alla "criminalità grave". Il limite di tre anni nel massimo, individuato dall'art. 132 co. 3 cod. *privacy*, non pare infatti idoneo ad

Peraltro, non appare affatto scontato che, anche prima dell'intervento del Giudice europeo, le interpretazioni volte a consentire una libera circolazione dei dati da un procedimento penale ad un altro fossero dotate di una solida base giuridica. Il sospetto deriva dalla dubbia compatibilità di simili letture con la garanzia dei diritti fondamentali che presidiano la materia.

È chiaro, infatti, che nessuna soluzione prospettabile in materia di uso processuale dei dati sul traffico può sottrarsi al confronto con lo statuto costituzionale della *data retention*. Sul piano dell'ordinamento interno, la Corte costituzionale ha chiarito, già nel 1993, che l'ampiezza della tutela accordata dall'art. 15 Cost. «è sicuramente tale da ricomprendere fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica»[41]. È quindi pacifico che l'acquisizione e utilizzo dei dati esterni delle telecomunicazioni soggiacciono alla duplice garanzia della riserva assoluta di legge e della riserva di giurisdizione.

Come noto, la riserva di legge è prescritta anche dalle fonti internazionali e sovranazionali che tutelano il rispetto della vita privata e familiare e la riservatezza. Il riferimento è agli articoli 7 e 8 della CDFUE, posti a fondamento dell'orientamento della Corte di giustizia sulla *data retention* e, naturalmente, all'art. 8 CEDU[42].

Se è vero, come confermato dalla Corte di giustizia nel suo precedente del 2023, che ogni uso successivo dei dati costituisce una compressione dei diritti fondamentali del soggetto interessato, occorre che tale uso sia regolato e garantito da una disciplina legislativa in grado di bilanciare ragionevolmente i contrapposti interessi che vengono

esplicare la funzione selettiva che le sentenze della Corte di giustizia sembrano attribuire al criterio in parola. Esprime simili perplessità, ad esempio, S. Marcolini, *La* data retention *nei sistemi giuridici comunitario e italiano*, in R. Flor, S. Marcolini, *Dalla* data retention *alle indagini ad alto contenuto tecnologico*, cit., 51, il quale osserva che il limite è di un anno inferiore a quello individuato per i casi di rito monocratico a citazione diretta, *ex* art. 550 Cpp.

[41] Così C. cost., 26.2.1993 n. 81, in *www.cortecostituzionale.it*; cfr. F.R. Dinacci, *L'acquisizione dei tabulati telefonici*, cit., 302 s., il quale ritiene inoltre che le prerogative sulle quali incide la *data retention* trovino tutela anche a norma dell'art. 14 Cost.

[42] In argomento, cfr. O. Pollicino, M. Bassini, sub *Art. 8*, in *Carta dei diritti fondamentali dell'Unione europea*, a cura di R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, 132 ss.; V. Zeno Zencovich, sub *Art. 8*, in *Commentario alla Convenzione Europea per la Tutela dei Diritti dell'Uomo e delle Libertà Fondamentali*, a cura di S. Bartole, B. Conforti, G. Raimondi, Padova 2001; nonché, da ultimo, M. Villiger, *Handbook on the European Convention on Human Rights*, Leiden 2023, 629 ss. Con riferimento a tali fonti, in tema di rapporto tra processo penale e nuove tecnologie, v. M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., 56 ss., il quale sottolinea che è in particolare l'art. 8 della Carta a garantire una protezione abbastanza avanzata della riservatezza, pur con il non trascurabile problema dell'assenza di una chiara riserva di giurisdizione. Ciò nonostante, come pure si osserva nel contributo citato richiamando le sentenze *Digital Rights* e *Prokuratuur*, la Corte di giustizia ha in più occasioni ritenuto necessario l'intervento dell'autorità giudiziaria in relazione ad atti idonei a incidere sulle garanzie coperte dalla disposizione in discorso.

in rilievo. Ciò tenendo a mente che «[r]iserva di legge vuol dire – quando è in gioco la tutela di diritti fondamentali, tra i quali il diritto alla riservatezza delle comunicazioni – che è vietato tutto ciò che non è espressamente consentito»[43].

Occorre quindi domandarsi se esista allo stato, in ambito nazionale, una disciplina che consenta e regoli la "circolazione" dei dati in altri procedimenti e, in caso affermativo, se essa sia conforme alle norme sovraordinate vigenti in materia.

È il caso di precisare che il problema non dovrebbe porsi quando ci si trovi ancora nei termini previsti per la conservazione. In tale ipotesi, infatti, il pubblico ministero potrà semplicemente procedere a norma dell'art. 132 cod. *privacy*, richiedendo al giudice l'autorizzazione all'acquisizione dei dati presso i gestori. Ciò, naturalmente, a condizione che si proceda per reati che ammettono il ricorso allo strumento investigativo in parola. La questione assume invece particolare rilievo nei casi in cui, in relazione ai dati utili per l'accertamento, ritualmente acquisiti nel primo procedimento, sia scaduto il termine di conservazione.

6.1. Il primo approdo della ricerca di una base legale per l'uso "obliquo" dei dati nel procedimento penale non può che essere l'art. 132 cod. *privacy*.

Come noto, alla disposizione in parola è affidata l'intera disciplina della *retention* e dell'accesso ai dati a fini di accertamento penale. Si tratterebbe, dunque, della sede "naturale" ove rintracciare un eventuale appiglio normativo idoneo a consentire la trasmigrazione delle informazioni al di fuori del procedimento di prima acquisizione.

Tuttavia, l'art. 132, che pure disciplina espressamente il momento acquisitivo del tabulato, rimane del tutto silente rispetto al trasferimento del medesimo ad altre sedi procedimentali[44].

Non sembra neppure possibile prospettare un'interpretazione analogica di tale disposizione. Anche ammettendo che la lacuna non sia intenzionale, occorre comunque riconoscere la natura eccezionale della previsione, la quale consente una serie di attività (conservazione dei dati e successivo accesso) incisive sui diritti fondamentali degli individui, al contempo, doverosamente, delimitandone i confini. Il disposto dell'art. 132 è dunque il risultato di un difficile bilanciamento delle

[43] In questi termini, G. Leo, *Le indagini sulle comunicazioni*, cit., 2; v. anche, sul tema, F.R. Dinacci, *I modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, in *www.archiviopenale.it*, 1/2024, 10, il quale sottolinea che, stante l'obbligo derivante (anche) dalle fonti europee di rispettare una riserva di legge, «se non disciplinato l'atto non può essere realizzato».

[44] A tal riguardo, cfr. A. Pasta, *Luci e ombre nella disciplina dei tabulati nel processo penale*, in *CP* 2022, 4460.

contrapposte esigenze di accertamento dei reati e di tutela della riservatezza, imposto dal rango degli interessi in gioco[45]. Non sembrano quindi persuasive le letture volte a ricavare, in sede interpretativa, la legittimità di compressioni dei diritti fondamentali degli individui ulteriori rispetto a quelle espressamente previste dalla legge.

Sull'eccezionalità della *data retention*, del resto, le indicazioni che provengono dal sistema europeo non lasciano alcun dubbio. Il già richiamato art. 15 della direttiva 2002/58/CE, che consente la conservazione e l'accesso ai dati entro i limiti indicati dalla norma e ampiamente integrati dalla Corte di giustizia, non costituisce che una deroga al divieto generale di conservazione di cui all'art. 5 della stessa direttiva.

Appurato che l'art. 132 cod. *privacy* non pone una disciplina della circolazione dei dati e che tale disposizione non ammette alcuna estensione oltre i casi espressamente previsti, sembra opportuno rivolgere altrove l'attenzione, allo scopo di verificare se vi siano altre norme in grado di supplire al segnalato vuoto di disciplina. Ciò sempre nel tentativo di individuare una disciplina dell'uso "secondario" dei dati compatibile con i rilevanti principi costituzionali e sovranazionali, in assenza della quale il fenomeno dovrà ritenersi vietato.

In tale prospettiva, sarà utile soffermarsi sulle principali soluzioni interpretative avanzate dalla dottrina e dalla giurisprudenza in tema di acquisizione e trasmigrazione dei dati sul traffico.

6.2. Merita qualche riflessione, a questo punto, l'orientamento che ammette l'utilizzo in altri procedimenti penali del tabulato contenente i dati ottenuti a norma dell'art. 132 cod. *privacy* attraverso i meccanismi che caratterizzano l'acquisizione dei documenti.

Occorre infatti considerare che è prevalente in giurisprudenza l'interpretazione volta ad inquadrare il tabulato nello schema giuridico della prova documentale[46]. Si tratta di una ricostruzione che trova parziale conforto anche in dottrina, laddove si osserva che il tabulato, costituito da una base materiale (cartacea o, più spesso, digitale) nella quale sono incorporate le informazioni relative al traffico telefonico e

[45] In argomento v., ad esempio, E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Padova 2018, 78 ss.

[46] V. Cass. 6.11.2014 n. 30897, Cass. 22.11.2007 n. 43329, cit.; Cass. 6.6.1995 n. 7994, in *OneLegale*. Cfr., sul punto, L. Tavassi, *Acquisizione di tabulati, tutela della* privacy *e rispetto del principio di proporzionalità*, in *www.archiviopenale.it*, 1/2022, 3, in cui si sottolinea che i dati fanno ingresso nel fascicolo del pubblico ministero e in quello del dibattimento come prove documentali.

telematico, integra gli elementi che concorrono a delineare la nozione di documento[47]. Sulla base di tale qualificazione, la giurisprudenza ritiene sufficiente, per la "trasmigrazione" del tabulato da un procedimento ad un altro, l'acquisizione a norma dell'art. 234 del codice di rito[48].

La descritta soluzione sembra esporsi a due critiche: una legata al concetto stesso di prova documentale, l'altra che attiene invece a considerazioni di ordine costituzionale.

A ben vedere, infatti, non appare del tutto scontato che il tabulato rientri nella nozione processuale di documento nel procedimento nell'ambito del quale viene acquisito. È pur vero che i requisiti configurati dall'art. 234 Cpp sembrerebbero integrati. Tuttavia, come noto, occorre distinguere tra documenti formati al di fuori del procedimento, suscettibili di essere inquadrati nella disciplina di cui all'art. 234, e la documentazione degli atti del procedimento[49].

La distinzione – che, per quanto interessa in questa sede, ha conseguenze decisive in materia di circolazione della prova – non è sempre agevole. A tal riguardo, l'orientamento consolidato della Cassazione è nel senso di ritenere necessarie, ai fini della qualifica di prova documentale, due condizioni: «a) che il documento risulti materialmente formato fuori, ma non necessariamente prima, del procedimento; b) che lo stesso oggetto della documentazione extraprocessuale appartenga al contesto del fatto oggetto di conoscenza giudiziale e non al contesto del procedimento»[50]. Secondo un criterio definito "teleologico", poi, non rileverebbe solo la collocazione dell'atto nella sequenza procedimentale, ma anche la sua destinazione[51].

I richiamati principi possono fornire qualche indicazione in ordine alla qualificazione del fenomeno in discorso. È pur vero che i dati vengono raccolti in una fase in cui potrebbero non essere ancora sorti indizi di reato a carico del titolare,

[47] In questo senso, ancora, E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori"*, cit., 35 ss., la quale ritiene che l'attività di acquisizione dei dati si configuri, sul piano dinamico, come «mezzo di assicurazione reale in funzione probatoria» e, su quello statico, come prova precostituita di carattere critico-indiziario; in senso conforme F. Zacché, *Acquisizione dei dati esterni ai colloqui telefonici*, in *DPP*, 3/1999, 339.

[48] È l'impostazione adottata, ad esempio, in Cass. 22.11.2007 n. 43329, cit.

[49] Cfr., in proposito, *Relazione prog. prel. c.p.p.*, in *G.U.*, 24.10.1998, n. 250, *Suppl. Ord.* n. 93, 66; sul tema v., per tutti, G. Ubertis, *Sistema di procedura penale,* vol. II*, Persone, strumenti, riti*, Milano 2023, 227 ss.

[50] Si tratta dell'orientamento condiviso dalla nota sentenza Cass. S.U. 28.3.2006, *Prisco*, in *RIDPP* 2006, 1537, con nota di A. Camon, *Le sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*. La distinzione era già stata proposta dai precedenti costituiti da Cass. 13.4.1999 n. 6887, *Gianferrari* e Cass. 16.3.1999 n. 5337, *Di Marco*.

[51] V., sul punto, R. Orlandi, *Atti e informazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, Milano 1992, 37, il quale fa riferimento ad alcune sentenze costituzionali, in particolare, C. cost., sentenze 27.11.1969 n. 149, 20.4.1988 n. 469 e 26.09.1990 n. 434, in *www.cortecostituzionale.it*.

avendo il legislatore optato per una conservazione generalizzata nei confronti di tutti gli utenti, per un periodo di tempo molto significativo. Si tratta, a ben vedere, di uno dei profili di maggiore delicatezza della disciplina italiana sulla *data retention*, ad elevatissimo rischio di incompatibilità con i principi affermati dalla Corte di giustizia[52].

È però altrettanto indiscutibile che, nonostante il grande anticipo con il quale si impone la raccolta di informazioni, si tratti di una conservazione connotata da una precipua funzione probatoria nel procedimento penale. Del resto, salvo il breve periodo necessario ai fini della fatturazione, la conservazione dei dati sarebbe del tutto vietata – se non altro a norma dell'art. 5 della direttiva 2002/58/CE – ove non fosse orientata a uno degli obiettivi indicati dal successivo art. 15. Ed è proprio l'esigenza di accertamento dei reati a costituire la base giuridica legittimante la *retention* prevista dall'art. 132 cod. *privacy*. Non si può dunque negare la vicinanza al contesto procedimentale del meccanismo di conservazione dei dati, orientato al successivo accesso, di cui all'art. 132.

Anche alla luce di simili considerazioni si spiegano le posizioni di coloro che individuano nella *data retention* un nuovo mezzo di ricerca della prova, ulteriore rispetto a quelli disciplinati dal codice di rito[53].

Le considerazioni appena proposte dovrebbero indurre, in sede interpretativa, ad escludere il tabulato dalla disciplina dell'art. 234 del codice di rito. Tale conclusione pare imporsi, d'altra parte, ove si consideri che l'interpretazione che consente l'acquisizione dei tabulati in altri procedimenti a norma della citata disposizione presta il fianco a seri dubbi di legittimità costituzionale.

Infatti, si ravvisa in tale disciplina un rilevante *deficit* di garanzie, inconciliabile con le esigenze di tutela che si pongono con riferimento all'utilizzo dei dati sul traffico[54]. Ciò era già emerso con particolare evidenza in relazione al momento acquisitivo, che secondo i numerosi arresti della Corte di giustizia deve essere presidiato, tra l'altro, dal

[52] Sul tema cfr., ad esempio, G. Lasagni, *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della* privacy, in *www.lalegislazionepenale.eu*, 3/2022, 131, in cui si afferma che «la mera previsione di termini di conservazione non è di per sé sufficiente a rendere una normativa rispettosa del principio di proporzionalità, né, quindi, a legittimare automaticamente tutte le conseguenti restrizioni al diritto di riservatezza».

[53] Così S. Marcolini, *La* data retention *nei sistemi giuridici comunitario e italiano*, cit., 45, il quale sottolinea come il fenomeno di cui si tratta necessiti di «procedure chiare, precise e munite di adeguate sanzioni, a protezione del bene della riservatezza che il mezzo inevitabilmente comprime».

[54] V., sul tema, F.R. Dinacci, *L'acquisizione dei tabulati telefonici*, cit., 312, il quale sottolinea che le recenti sentenze della Corte di giustizia hanno posto in evidenza i profili di incompatibilità dell'acquisizione del tabulato con lo schema giuridico della prova documentale, facendo propendere per l'attrazione del fenomeno nella disciplina della segretezza delle comunicazioni.

rispetto del principio di proporzionalità e dal correlativo controllo del giudice. Proprio tali profili di incompatibilità hanno "costretto" il legislatore a prevedere una disciplina differenziata per l'acquisizione dei dati.

Se il contrasto esiste con riguardo all'acquisizione del tabulato, sembra lecito dubitare che la disciplina sui documenti sia invece applicabile senza difficoltà al suo trasferimento in altri procedimenti. Del resto, lo si ribadisce, la sentenza della Corte di giustizia sul caso *A.G.* sembra indicare che gli stessi problemi che si pongono in relazione alla prima acquisizione del tabulato valgono anche per gli usi successivi dei dati, parimenti idonei a compromettere i diritti fondamentali – protetti dagli articoli 7 e 8 della Carta – degli individui ai quali si riferiscono.

Le medesime considerazioni paiono imporsi alla luce dell'art. 15 Cost., che – nel porre la riserva di legge assoluta – prevede che la limitazione della libertà e segretezza della corrispondenza può avvenire soltanto «con le garanzie stabilite dalla legge»[55]. Tali garanzie non sembrano potersi ravvisare nella disposizione di cui all'art. 234 Cpp, la quale si limita a consentire l'acquisizione di documenti che rappresentano fatti rilevanti per l'accertamento penale.

Tale ricostruzione sembra trovare conforto in una recente e ben nota pronuncia della Consulta, resa in tema di acquisizione di corrispondenza elettronica[56]. In tale occasione, la Corte ha ritenuto che «degradare le comunicazioni a mero documento quando non più *in itinere*» finirebbe per azzerare la tutela costituzionale dell'art. 15 con riferimento alle modalità di messaggistica elettronica. Così argomentando, il Giudice delle leggi pare confermare la mancanza, nell'art. 234 Cpp, del corredo di garanzie costituzionalmente necessarie in materie coperte dall'art. 15 Cost[57].

La riconducibilità all'art. 234 Cpp dell'attività di acquisizione e trasferimento dei dati, già non pacifica dal punto di vista processuale, dovrebbe quindi essere esclusa

[55] Cfr., al riguardo, F. Donati, sub *Art. 27*, in *Commentario alla Costituzione*, a cura di R. Bifulco, A. Celotto, M. Olivetti, Torino 2006, 368, in cui si sottolinea il carattere assoluto della riserva di legge formale, in forza della quale il legislatore deve stabilire garanzie ulteriori rispetto all'atto motivato dell'autorità giudiziaria.

[56] C. cost., 22.6.2023 n. 170, in *www.cortecostituzionale.it*, sulla quale v., fra i molti, F. Cerqua, L. Lupária, *La versione della Consulta sulla corrispondenza elettronica. Un* bouleversement *in materia di prova digitale*?, in *Dir. inf.* 2023, 718 ss.; R. Orlandi, *"Corrispondenza" dei parlamentari e limiti all'accertamento penale. Appunti critici sulla sentenza nr. 170 del 2023 della Corte costituzionale*, *ivi*, 730 ss.; G. Spangher, *Dopo i parlamentari servono garanzie per gli imputati*, *ivi*, 742 ss.; G. Guzzetta, *La nozione di comunicazione e altre importanti precisazioni della Corte costituzionale sull'art. 15 della Costituzione nella sentenza n. 170 del 2023*, in *www.federalismi.it*, 21/2023, 81 ss.; F.R. Dinacci, *I modi acquisitivi della messaggistica chat o e-mail*, cit., 13 ss.

[57] In argomento, G. Guzzetta, *La nozione di comunicazione e altre importanti precisazioni della Corte costituzionale*, cit., 84 ss.; F. Cerqua, L. Lupária, *La versione della Consulta sulla corrispondenza elettronica*, cit., 725.

alla luce delle esposte ragioni di carattere costituzionale.

6.3. Ove si volesse accogliere la prospettiva che accosta la *data retention* all'attività di indagine, ci si dovrebbe domandare se il tabulato possa circolare a norma dell'art. 238 co. 3 del codice di rito, che si riferisce all'acquisizione di documentazione relativa ad atti irripetibili[58].

Anche tale soluzione pare tuttavia impercorribile. La richiamata disposizione prevede infatti che, in caso di irripetibilità sopravvenuta, la documentazione possa essere acquisita solo qualora questa sia dovuta a fatti o circostanze imprevedibili. Nel caso in esame, l'irripetibilità, dovuta al decorso dei termini di cui all'art. 132 cod. *privacy*, sarebbe tutt'altro che imprevedibile: essa conseguirebbe anzi a un divieto di acquisizione espressamente stabilito dalla legge. Divieto che, oltretutto, costituisce niente meno che l'espressione del bilanciamento legislativo volto a contemperare le esigenze di accertamento con la grave compressione dei diritti fondamentali dell'individuo.

Davvero assorbente pare poi, anche in questo caso, l'argomento fondato sulla dubbia compatibilità costituzionale di una simile interpretazione. Gli stessi rilievi formulati con riguardo all'impostazione che ritiene applicabile l'art. 234 Cpp, relativi al *deficit* di garanzia rispetto agli *standard* richiesti dall'art. 15 della Costituzione, potrebbero essere riproposti anche con riguardo all'art. 238 del codice.

È pur vero che la norma in discorso è preordinata alla circolazione probatoria e, dunque, pone al riguardo una disciplina più articolata rispetto a quella delineata dall'art. 234. Tuttavia, non sembra possibile rintracciare nella disposizione citata quelle garanzie che dovrebbero corredare la disciplina di un fenomeno che incide sulle prerogative tutelate dall'art. 15 della Costituzione.

Neppure le norme sulla circolazione dei verbali di prove di altri procedimenti paiono quindi idonee ad offrire una base giuridica idonea a regolare l'uso "secondario" dei dati nei procedimenti penali.

6.4. Nella prospettiva del ragionamento fin qui delineato, non può infine mancare il riferimento alla disciplina della circolazione delle intercettazioni telefoniche. Infatti,

[58] Sull'irripetibilità degli atti e sul regime della circolazione cfr., per tutti, C. Cesari, *"Giusto processo", contraddittorio ed irripetibilità degli atti di indagine*, in *RIDPP* 2001, 56 ss., A. Gaito, *La circolazione delle prove e delle sentenze*, in *www.archiviopenale.it*, 3/2011, 9; P. Tonini, C. Conti, *Il diritto delle prove penali*, Milano 2014, 396 ss.

tra l'attività intercettiva e la raccolta dei dati sul traffico sussistono elementi di significativa "familiarità"[59].

È diffusa, soprattutto nell'ordinamento interno, l'opinione secondo la quale l'acquisizione dei dati sul traffico si collocherebbe su un gradino più basso, rispetto alle intercettazioni, in una scala di intrusività nella sfera privata dei singoli[60]. L'assunto si fonda essenzialmente sull'inidoneità della *data retention* a cogliere il contenuto delle comunicazioni, al quale invece si accede con l'intercettazione di comunicazioni. Il rilevato divario di incisività varrebbe a giustificare un minor livello di garanzie nella disciplina della conservazione e dell'acquisizione dei dati di traffico.

Una simile ricostruzione non convince del tutto. L'analisi della grande mole di dati conservati può infatti restituire un quadro molto preciso delle abitudini di vita, degli spostamenti, delle opinioni e addirittura della personalità dell'interessato[61]. Ciò in ragione della tipologia e quantità di informazioni rese disponibili dallo strumento investigativo in discorso, fra le quali rientrano i dati sulle comunicazioni telefoniche, sulla localizzazione geografica del dispositivo tramite l'individuazione delle celle telefoniche "agganciate", sul traffico telematico e sulla navigazione in *Internet*[62].

Per certi versi, dunque, l'intrusività dell'attività di raccolta di metadati potrebbe addirittura risultare superiore rispetto a quella che connota l'intercettazione telefonica. In tale prospettiva, si è sottolineato che le persone sono tendenzialmente in grado di controllare le proprie affermazioni o utilizzare un linguaggio cifrato

[59] In questo senso, in particolare, E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori"*, cit., 3, la quale sottolinea la particolare intensità del legame tra intercettazioni e *data retention*; sul tema, v. anche G. Leo, *Le indagini sulle comunicazioni*, cit., 4 ss., per una ricostruzione del rapporto tra *data retention* e disciplina delle intercettazioni, con ampi riferimenti giurisprudenziali.

[60] In questo senso, ad esempio, Cass. S.U. 8.5.2000 n. 6, in *OneLegale*.

[61] In questo senso, L. Lupária, Data retention *e processo penale*, cit., 758, il quale sottolinea come la raccolta di dati di traffico telefonico e telematico consenta di tracciare un profilo del carattere della persona alla quale i dati si riferiscono e di mapparne gli spostamenti; M. Daniele, *La prova digitale nel processo penale*, cit., 288; I. Neroni Rezende, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *www.sistemapenale.it*, 5/2020, 195 s. Tali aspetti di delicatezza, finora non compiutamente colti dalla prevalente giurisprudenza interna, sono invece da tempo valorizzati dalla giurisprudenza di Lussemburgo e di Strasburgo. Oltre alle già citate sentenze della Corte di giustizia, si veda la nota sentenza della C. eur., 13.9.2018, *Big Brother Watch c. Regno Unito*, nn. 58170/13, 62322/14 e 24960/15.

[62] Cfr. L. Tavassi, *Acquisizione di tabulati,* cit., 3. Quanto ai c.d. *file* di *log*, particolarmente rilevanti in quanto idonei a rivelare tutte le attività compiute in *Internet* da un utente, sussiste qualche incertezza in merito alla disciplina applicabile. Se non vi sono dubbi sul fatto che i *file* di *log* relativi alle attività di comunicazione via *web* rientrino nella disciplina dell'art. 132 cod. *privacy*, non è invece chiaro se vi siano riconducibili anche i dati che riguardano la navigazione ma non le comunicazioni; sul tema, particolarmente problematico, v. J. Della Torre, A. Malacarne, *L'utilizzo dei* file *di* log *per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in *www.archiviopenale.it*, 3/2023, 9 ss.

nell'ambito di una telefonata, mentre la produzione di una grande quantità di dati di traffico è un fenomeno che sfugge dalla sfera di controllo dell'utente medio[63].

Su un piano più ampio, poi, pare opportuno ricordare ancora una volta che la raccolta dei dati riguarda la generalità delle persone, a prescindere dal loro coinvolgimento anche potenziale in vicende illecite, a differenza di quanto avviene con riferimento alle intercettazioni. La permanente sensazione di sorveglianza che ne deriva può condurre alla gravissima conseguenza di ostacolare o scoraggiare l'esercizio delle libertà fondamentali da parte degli individui[64]. La serietà dell'incidenza del fenomeno sugli interessi costituzionalmente protetti non può dunque essere sminuita.

Stante l'affinità delle istanze meritevoli di tutela, potrebbe apparire lecito domandarsi se la disciplina dettata con riferimento alla circolazione delle intercettazioni sia applicabile anche alla materia di cui si tratta. Un simile percorso ermeneutico era stato intrapreso in passato dalla giurisprudenza di legittimità, la quale aveva tentato di estendere la disciplina di cui agli artt. 266 e seguenti Cpp all'acquisizione dei tabulati[65]. Tuttavia, la soluzione è stata smentita dalla Corte costituzionale e abbandonata dalla giurisprudenza successiva[66].

L'estensione analogica delle norme sulle intercettazioni sembra in effetti preclusa dalle innegabili differenze che intercorrono tra i due istituti sotto il profilo tecnico e strutturale[67]. A tal riguardo, si è osservato, ad esempio, che l'attività intercettiva presuppone la captazione clandestina del contenuto delle comunicazioni nel loro divenire[68], il che non vale per la *data retention*.

Non per questo il riferimento all'art. 270 Cpp può ritenersi poco pertinente[69]. Al

[63] Così G. Lasagni, *Dalla riforma dei tabulati a nuovi modelli di integrazione*, cit., 14 s.; nello stesso senso G. Leo, *Le indagini sulle comunicazioni*, cit., 5. Occorre considerare, altresì, che i dati così raccolti possono essere efficacemente esaminati da *software* in grado di effettuarne una lettura incrociata, come sottolineato da I. Neroni Rezende, *Dati esterni alle comunicazioni*, cit., 195.

[64] Sul punto cfr. E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori"*, cit., 9 s.

[65] Per tutte, Cass. S.U. 24.10.1998 n. 21, in *OneLegale*.

[66] C. cost., 7.7.1998 n. 281, in *www.cortecostituzionale.it*, in cui si afferma che l'intervento richiesto dal rimettente comporterebbe «il trapianto di un frammento della specifica disciplina dell'intercettazione telefonica al diverso istituto dell'acquisizione dei tabulati»; l'equiparazione normativa dei due istituti era già stata esclusa dalla già citata sentenza n. 81 del 1993.

[67] In questo senso, E. Andolina, *L'acquisizione nel processo penale dei dati "esteriori"*, cit., 5 s.

[68] Così F. Caprioli, *Colloqui riservati e prova penale*, Torino 2000, 172 s., il quale, pur riconoscendo le affinità tra gli atti *strictu sensu* intercettivi e quelli che consentono di apprendere il contenuto di una comunicazione a posteriori, ritiene che le differenze strutturali non consentano un'estensione della disciplina delle intercettazioni.

[69] Sul tema v., per tutti, V. Grevi, *La nuova disciplina delle intercettazioni telefoniche*², Milano 1982, 60 ss.; G. Illuminati, *La disciplina processuale delle intercettazioni*, Milano 1983, 163 ss.; A. Camon, *Le intercettazioni nel*

contrario, nel dibattito dottrinale e nell'evoluzione giurisprudenziale che hanno riguardato la norma menzionata possono rintracciarsi le coordinate per una razionale ricostruzione della disciplina dell'acquisizione dei dati esterni delle telecomunicazioni in procedimenti penali differenti. È noto che l'art. 270 pone il divieto di utilizzazione delle intercettazioni in procedimenti diversi da quelli nei quali sono state disposte, indicando i casi in cui è consentita la circolazione. Preme sottolineare che il divieto con cui si apre la disposizione è espressione di un principio generale, mentre l'ipotesi di "trasmigrazione" del captato dovrebbe ritenersi del tutto eccezionale[70].

Tale principio generale, pur in parte messo in discussione dalla più recente riforma dell'art. 270[71], sembra discendere direttamente dalla cornice costituzionale in cui si inserisce la disciplina *de qua*. Il diritto «inviolabile» alla libertà e segretezza delle comunicazioni può essere limitato, come detto, solo in forza di una legge che preveda le dovute «garanzie» e per «atto motivato dell'autorità giudiziaria». La Corte costituzionale ha chiarito che tale libertà «risulterebbe pregiudicata, gravemente scoraggiata o, comunque, turbata ove la sua garanzia non comportasse il divieto di divulgazione o di utilizzazione successiva delle notizie di cui si è venuti a conoscenza a seguito di una legittima autorizzazione di intercettazioni al fine dell'accertamento in giudizio di determinati reati»[72]. I limiti entro i quali è consentito comprimere la prerogativa di cui all'art. 15 sono posti, all'esito del delicato bilanciamento degli interessi in gioco, dalla legge, la quale non può certo ammettere che il primo provvedimento del giudice assuma la valenza di «un'inammissibile autorizzazione in bianco»[73].

Per tale via si valorizza altresì, quale indispensabile presidio legittimante l'uso delle

processo penale, Milano 1996, 271 ss.; L. Filippi, *L'intercettazione di comunicazioni*, Milano 1997, 180 ss.

[70] Cfr. A. Gaito, *La circolazione delle prove e delle sentenze*, cit., 17; J. Della Torre, *La nuova disciplina della circolazione del captato: un nodo arduo da sciogliere*, in *Diritto di Internet*, supplemento al fascicolo 3-2020, a cura di M. Gialuz, 90; A. Malacarne, *L'art. 270 comma 1 cpp al crocevia fra interpretazioni giurisprudenziali ed interventi normativi*, in *www.lalegislazionepenale.eu*, 3.6.2020, 2.

[71] Oggi, la circolazione dei risultati delle intercettazioni è vietata a meno che non risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza o dei reati di cui all'articolo 266 co. 1. Tale è la formulazione della disposizione all'esito delle modifiche di cui alla l. 28.2.2020 n. 7. Per la dottrina prevalente, l'interpretazione più garantista, secondo la quale la circolazione sarebbe ammessa soltanto in relazione a reati che rientrino in entrambe le menzionate categorie, attribuendo alla «e» un valore condizionale, è difficilmente sostenibile. Cfr., anche per gli opportuni riferimenti bibliografici, E. Valentini, *Un rompicapo senza fine: le arcane trasformazioni dell'art. 270 c.p.p.*, in *Revisioni normative in tema di intercettazioni*, a cura di G. Giostra, R. Orlandi, Torino 2021, 300 ss. Per i dubbi di legittimità costituzionale della disposizione così interpretata cfr. *infra*, n. 92.

[72] Così C. cost., 11.7.1991 n. 366, in *www.cortecostituzionale.it*.

[73] Ancora, C. cost., 11.7.1991 n. 366, cit. alla nota precedente.

intercettazioni, la riserva di giurisdizione. Infatti, ammettere la libera circolazione del captato eluderebbe la garanzia costituzionale della motivazione, giacché il vaglio sui presupposti di legittimità dell'attività intercettiva sarebbe svolto solo nel diverso procedimento nell'ambito del quale è stata disposta la prima acquisizione e riferito soltanto a tale contesto[74]. Ed è proprio il provvedimento autorizzativo motivato che garantisce che «siano quantomeno predeterminati sia i soggetti da sottoporre al controllo, sia i fatti costituenti reato per i quali in concreto si procede»[75].

La necessità costituzionale del divieto generale di cui si tratta è ulteriormente confermata dal Giudice delle leggi, laddove afferma che il principio è derogabile soltanto all'esito «del più rigoroso scrutinio» volto a verificare «se la restrizione prevista sia diretta al soddisfacimento di un interesse pubblico primario costituzionalmente rilevante e, nello stesso tempo, risulti circoscritta alle operazioni strettamente necessarie alla tutela di quell'interesse»[76]. Se, come chiarito dalla Corte, è la norma che consente l'utilizzo *aliunde* ad essere eccezionale, in quanto incidente su un diritto inviolabile, la conseguenza appare ineludibile: ove non esistesse l'art. 270 Cpp, la circolazione del captato sarebbe vietata[77].

Sembra d'altra parte che i principi appena ricordati debbano valere anche per i dati esterni delle telecomunicazioni. Non pare più sostenibile, infatti, la tesi secondo la quale il divario intercorrente tra il livello di lesività delle intercettazioni e della *data retention* sia tale da giustificare significative disparità di trattamento nella regolamentazione dei due fenomeni. Peraltro, anche a prescindere dal dibattito sulla maggiore o minore pervasività del mezzo, la sola ricomprensione nell'alveo dell'art. 15 Cost., oltre che degli artt. 7 e 8 della Carta, sembra sufficiente a escludere la legittimità di una circolazione "sregolata" dei dati da un procedimento all'altro.

6.5. Come si è cercato di argomentare nelle pagine che precedono, la ricerca di una disciplina idonea a consentire e regolare l'uso "obliquo" dei dati nell'ambito di procedimenti penali non appare al momento destinata ad avere un esito favorevole.

---

[74] L. Filippi, *L'intercettazione di comunicazioni*, cit., 182; cfr. anche, sul tema, A. Camon, *Le intercettazioni nel processo penale*, cit., 275, il quale osserva che, se adeguatamente motivato, il provvedimento autorizzativo non può dirsi carente nella motivazione sulla base di un'analisi *ex post*.

[75] Il riferimento è sempre a C. cost., 11.7.1991 n. 366, cit.

[76] In questi termini, C. cost., 10.2.1994 n. 63, in *www.cortecostituzionale.it*; sottolinea questi aspetti J. Della Torre, *La nuova disciplina della circolazione del captato*, cit., 91.

[77] Non può quindi essere condivisa la posizione di chi legge nell'art. 270 un limite alla possibilità di utilizzare le intercettazioni in altri procedimenti.

Infatti, l'art. 132 cod. *privacy*, norma che disciplina per intero il fenomeno acquisitivo dei dati sul traffico, tace al riguardo. Le ragioni di ordine costituzionale e processuale sopra esposte paiono poi condurre ad escludere l'applicabilità degli artt. 234 e 238 del codice di rito. L'art. 270 Cpp, che sembrerebbe idoneo a garantire un maggiore livello di garanzie, non pare invece applicabile in considerazione delle differenze strutturali che intercorrono tra le intercettazioni e il fenomeno della *data retention*.

Ragioni di legalità processuale e, soprattutto, la vigenza in materia di una riserva assoluta di legge inducono a ritenere che, mancando una disciplina della circolazione dei dati, questi debbano rimanere all'interno del procedimento nell'ambito del quale sono stati acquisiti.

Dalle considerazioni appena espresse vanno dunque tratte le dovute conclusioni con riferimento ai procedimenti penali in corso, nell'ambito dei quali siano stati trasferiti i tabulati acquisiti *aliunde*. Il contrasto con le richiamate fonti sovraordinate induce a chiamare in causa il concetto di "prova incostituzionale"[78]. Al riguardo, già nel 1973, la Corte costituzionale ha affermato, proprio in riferimento all'art. 15 Cost., che «attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito»[79].

Come noto, la conseguenza riconnessa, sul piano processuale, alla violazione dei diritti fondamentali è l'inutilizzabilità della "prova incostituzionale" [80]. Simili argomenti sono stati addotti con riferimento alla rilevata incompatibilità della disciplina interna sull'acquisizione dei dati con le fonti sovranazionali, come interpretate dalla Corte di giustizia[81]. Sembra che il principio debba valere anche in materia di uso "secondario" dei dati, laddove si ravvisi una violazione delle norme costituzionali.

Secondo questa linea interpretativa, nei giudizi in corso andrebbe rilevata l'inutilizzabilità patologica dei tabulati provenienti da altri procedimenti.

Conclusioni in parte analoghe potrebbero imporsi alla luce del principio del rimedio

[78] Sul tema, per tutti, V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche illegittime*, in *GCos* 1973, 341 ss.; A. Camon, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove «incostituzionali»*, in *CP* 1999, 1188 ss.; F.R. Dinacci, *L'inutilizzabilità nel processo penale*, Milano 2008, 75 ss.; C. Conti, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *DPP* 2018, 1210 ss.

[79] Il riferimento è a C. cost., 4.4.1973 n. 34, in *www.cortecostituzionale.it*.

[80] Cfr., ad esempio, C. Conti, *Prova informatica e diritti fondamentali*, cit., *loc. ult. cit.*

[81] Così F.R. Dinacci, *L'acquisizione dei tabulati telefonici*, cit., 308 ss.

effettivo, di cui all'art. 47 della Carta[82]. Una parte degli interpreti ritiene infatti ipotizzabili, in ossequio al menzionato principio, delle ipotesi di invalidità processuale quando una disposizione interna violi il diritto dell'Unione[83]. Tale sembra l'impostazione adottata dalla Corte, ad esempio, nella sentenza *Prokuratuur*, in cui si afferma che «il principio di effettività impone al giudice penale nazionale di escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati»[84].

Nella delineata prospettiva, la lesione degli artt. 7 e 8 della Carta potrebbe trovare rimedio nella dichiarazione di invalidità degli atti probatori compiuti in violazione dei criteri specificati dalla Corte di giustizia in materia di uso "secondario" dei dati.

Per il tramite delle soluzioni appena tratteggiate, potrebbe essere neutralizzato il rischio di un pregiudizio delle prerogative costituzionalmente tutelate degli imputati nei procedimenti pendenti, derivante dall'acquisizione di materiale probatorio in violazione dei principi fondamentali che regolano la materia. I rimedi richiamati non varrebbero, invece, con riferimento ai procedimenti già definiti con sentenza irrevocabile[85].

Occorre una precisazione riguardo ai tabulati contenenti informazioni favorevoli all'imputato. Le ipotesi di inutilizzabilità prospettate non potrebbero applicarsi *contra reum*, considerato che esse scaturiscono proprio dall'eventuale violazione dei diritti

[82] Sul principio del ricorso effettivo *ex* art. 47 CDFUE, v., da ultimo, quanto alla materia penale, C.G.UE, *Gavanozov*, 11.11.2021, C-852/19, ECLI:EU:C:2021:902, sulla quale v. A. Nascimbeni, *Ordine europeo di indagine penale e diritti fondamentali*, in *RIDPP* 2022, 591 ss.

[83] Sul tema, cfr. A. Cabiale, *I rimedi nelle direttive di Stoccolma: poche parole e molti silenzi*, in *RIDPP* 2018, 2143; Id., *I limiti alla prova nella procedura penale europea*, Milano 2019, 215 ss.; v. anche, al riguardo, J. Della Torre, *Le direttive UE sui diritti fondamentali degli accusati: pregi e difetti del primo "embrione" di un sistema europeo di garanzie difensive*, in *CP* 2018, 1413. Per F.R. Dinacci, *I modi acquisitivi della messaggistica chat o e-mail*, cit., 12, è configurabile, alla luce della giurisprudenza della Corte di giustizia, «un'inutilizzabilità di derivazione comunitaria», che si affianca a quelle derivanti dalla violazione delle norme costituzionali; nello stesso senso, S, Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *CP* 2015, 780 s.; L. Lupária, Data retention *e processo penale*, cit., 763, il quale osserva, peraltro, che la Cassazione non ha accolto tali spunti dottrinali in materia di inutilizzabilità "eurounitaria". Il riferimento è a Cass. 24.4.2018 n. 33851, in *OneLegale*.

[84] C.G.UE, *H.K* (*Prokuratuur*), cit., § 44.

[85] Il giudicato potrebbe essere messo in discussione per il tramite di un mezzo di impugnazione straordinario, ove il condannato riuscisse a conseguire una sentenza favorevole della Corte EDU che accerti la violazione dei diritti sanciti dalla Convenzione in conseguenza dell'uso "secondario" dei dati. Per tale soluzione, con riferimento all'acquisizione dei dati in violazione dei diritti fondamentali della parte, v. ancora S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale*, cit., 783 ss., il quale prospetta il ricorso alla "revisione europea" in caso di pronuncia di Strasburgo che accerti la violazione degli artt. 6 e 8 della Convenzione. Oggi, in tali ipotesi, sarebbe esperibile il nuovo mezzo di impugnazione di cui all'art. 628-*bis* Cpp.

fondamentali della parte. Tale *vulnus* non ricorre, naturalmente, in caso di uso *in bonam partem* dei dati sul traffico[86].

7. Con la riflessione sin qui condotta, si è tentato di fornire, in via interpretativa, una soluzione compatibile con le esigenze di tutela dei diritti fondamentali degli individui al tema dell'uso "obliquo" dei dati sul traffico, resa necessaria dal silenzio dell'ordinamento sul punto.

Pur essendo la lettura proposta riconducibile a principi costituzionali e sovranazionali che già da tempo costituiscono patrimonio del nostro sistema giuridico, si deve rilevare che, come spesso accade in materia di *data retention*, ancora una volta l'impulso decisivo per un innalzamento degli *standard* di tutela proviene da una sentenza della Corte di giustizia dell'Unione.

Nell'ambito dell'ordinamento interno, numerosi sono stati infatti i profili di tensione con le fonti sovranazionali, progressivamente posti in luce dalla giurisprudenza europea. Alcuni di essi – ad esempio, la necessità di affidare ad un'autorità indipendente e imparziale la decisione sull'accesso ai dati – sono stati superati dal legislatore. Su molti altri temi, come rilevato da più parti, il contrasto sembra permanere. Si pensi ai tempi della *retention*, che ha una durata prevista di 12 o 24 mesi – rispettivamente, per i dati sul traffico telematico e telefonico – ma in realtà arriva a 72 mesi in forza dell'art. 24 della l. 20.11.2017 n. 167[87], al carattere ancora generalizzato della conservazione[88], all'individuazione dei reati sulla sola base dell'indicazione di una soglia edittale di tre anni nel massimo[89] o alla mancata tutela

[86] Per A. Pasta, *Luci e ombre nella disciplina dei tabulati nel processo penale*, cit., 4461, «è difficile immaginare che qualcuno possa negare l'acquisizione di tabulati contenuti nel fascicolo di un altro procedimento nel caso in cui da esso si tragga la prova della non colpevolezza dell'accusato».

[87] La norma prevede che, in considerazione delle esigenze di contrasto del terrorismo, per le finalità di accertamento e repressione dei gravi reati indicati nella previsione, il termine di conservazione dei dati relativi al traffico telefonico e telematico e alle chiamate senza risposta è stabilito in 72 mesi, in deroga a quanto previsto dall'articolo 132. Risulta evidente che tutti i dati devono essere conservati per tale periodo di tempo estremamente esteso, non essendo possibile, allo stato, distinguere in anticipo quali informazioni potranno essere utili ai fini delle indagini di cui all'art. 24. Sul tema cfr., S. Signorato, *Novità in tema di* data retention. *La riformulazione dell'art. 132 codice* privacy *da parte del D.Lgs. 10 agosto 2018 n. 101,* in *www.penalecontemporaneo.it*, 28.11.2018, 156 s.; G. Lasagni, *Dalla riforma dei tabulati a nuovi modelli di integrazione*, cit., 9; G. Formici, *La disciplina della* data retention, cit., 333.

[88] Si tratta, storicamente, di uno dei punti dolenti della disciplina interna sulla *data retention*. Auspica una riforma che verta su tale profilo, da ultimo, L. Filippi, *La disciplina italiana dei tabulati telefonici e telematici*, cit.

[89] Si erano già espresse, in dottrina, perplessità sull'idoneità del criterio adottato dal legislatore italiano a individuare la categoria dei reati "gravi", per l'accertamento dei quali le fonti europee consentono la conservazione e l'accesso ai dati; sul tema, ad esempio, S. Marcolini, *La* data retention *nei sistemi giuridici*

dei terzi ai quali si riferiscono le informazioni acquisite[90].

Nel quadro così delineato la Corte di giustizia ha avuto altresì occasione di far emergere un ulteriore potenziale profilo di inadeguatezza della disciplina interna rispetto allo statuto sovranazionale della materia. Con la sentenza sul caso *A.G.*, si è infatti sottolineata l'incompatibilità con il diritto dell'Unione europea delle prassi, diffuse nel nostro ordinamento, alla stregua delle quali il tabulato, una volta acquisito in un procedimento penale, è ritenuto libero di circolare al pari di qualunque documento.

Tali letture, come detto, dovrebbero ora ritenersi bandite, quanto meno con riguardo ai procedimenti diversi da quelli che perseguono finalità di contrasto alla criminalità grave o, eventualmente, obiettivi di maggiore importanza nella gerarchia delineata dalla giurisprudenza europea. Anche con riferimento ai procedimenti rispetto ai quali la circolazione dei dati non è stata espressamente vietata dalla Corte occorre però un intervento del legislatore. Una volta chiarito che il trasferimento delle informazioni da una sede procedimentale ad un'altra incide sugli stessi interessi coinvolti nella prima acquisizione delle stesse, è necessario elaborare una disciplina legale che regoli il fenomeno, assicurando le dovute garanzie.

Alla luce della pronuncia in questione, un punto sembra incontrovertibile: la disciplina della quale si auspica l'introduzione non potrà consentire il trasferimento dei dati in procedimenti per reati meno gravi rispetto a quelli che ne ammettono, in prima battuta, l'acquisizione.

In ossequio al principio di proporzionalità, che anche in questa materia costituisce un vincolo ineludibile per il legislatore, sembra poi doversi dubitare della legittimità di una disciplina che consentisse sempre il trasferimento dei tabulati da un procedimento ad un altro, con il solo limite indicato dall'art. 132 cod. *privacy* quanto alla gravità del reato.

È pur vero che si tratterebbe di una previsione in linea con l'attuale versione dell'art. 270 Cpp, secondo l'interpretazione oggi prevalente di tale disposizione[91]. Tuttavia, paiono cogliere nel segno le critiche di chi ha ravvisato nel *novum* normativo in

comunitario e italiano, cit., 51. Sul tema è intervenuta, di recente, C.G.UE, Grande Sezione, 30.4.2024, C-178/22, cit., prendendo in esame proprio la disciplina italiana. Con tale decisione la Corte ha affermato che il diritto dell'Unione non osta ad una soluzione normativa quale quella adottata dal legislatore italiano, a patto che al giudice sia consentito negare l'accesso «se quest'ultimo è richiesto nell'ambito di un'indagine vertente su un reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato».

[90] Al riguardo, cfr. L. Tavassi, *Acquisizione di tabulati,* cit., 11 ss.

[91] V. *supra*, par. 6.4.

questione un vistoso arretramento rispetto al livello di garanzie che sembrerebbe imporsi alla luce delle già richiamate pronunce del Giudice delle leggi[92].

Invero, il principio secondo il quale, in materie coperte dall'art. 15 Cost., il divieto di circolazione dovrebbe essere la regola e la trasmigrazione l'eccezione, ritenuto dalla Corte costituzionale un fondamentale presidio posto a tutela della libertà delle comunicazioni, non sembra poter essere messo da parte.

Sul piano della tutela della riservatezza, occorre poi considerare che l'uso "obliquo" dei dati costituisce una "perpetuazione" dell'ingerenza, provocandone un'estensione dal punto di vista temporale e determinando una moltiplicazione delle sedi di possibile impiego delle informazioni, senza dimenticare che è in gioco anche la riservatezza dei terzi ai quali i dati si riferiscono.

Sarebbe dunque auspicabile un intervento legislativo orientato in direzione opposta rispetto a quella intrapresa con la recente modifica dell'art. 270 del codice di rito e pertanto volto a individuare i casi nei quali l'importanza degli obiettivi di accertamento perseguiti rendano legittima e opportuna un'ulteriore compressione dei diritti fondamentali degli individui[93]. Si consideri, inoltre, che l'art. 270 potrebbe oggi essere posto in discussione anche alla luce della recente pronuncia della Grande Sezione che ha prescritto, in materia di acquisizione dei dati sul traffico, il vaglio di proporzionalità in concreto del giudice circa la gravità del reato per il quale si procede[94].

Una nuova disciplina della circolazione dei dati sul traffico presupporrebbe dunque,

---

[92] In tal senso, L. Filippi, *Intercettazioni:* habemus legem!, in *DPP* 2020, 462; J. Della Torre, *La nuova disciplina della circolazione del captato*, cit., 99 s., il quale sottolinea come la nuova formulazione dell'art. 270 paia delineare un «regime di circolazione delle captazioni palesemente confliggente con la Carta fondamentale, per come interpretata dalla Corte costituzionale»; E. Valentini, *Un rompicapo senza fine*: *le arcane trasformazioni dell'art. 270 c.p.p.*, cit., 308 ss.

[93] Sarebbe anche auspicabile, sempre nella prospettiva di un più completo adeguamento ai principi fondamentali, un provvedimento motivato nel quale il giudice dia conto della valutazione di proporzionalità in concreto compiuta in relazione al trasferimento. Peraltro, è il caso di sottolineare che la Corte costituzionale ha in passato ritenuto legittimo il meccanismo di trasferimento previsto *ex* art. 270 Cpp anche in assenza di un nuovo atto motivato dell'autorità giudiziaria, a condizione che si tratti di un'eventualità eccezionale e proporzionata. In tal senso, ad esempio, la già citata sentenza n. 366 del 1991.

[94] Gli effetti della sentenza C.G.UE, Grande Sezione, 30.4.2024, C-178/22, cit., paiono potersi spiegare anche al di fuori del settore dell'acquisizione dei dati sul traffico. Cfr., sul tema, D. Albanese, *Dalla Corte di giustizia dell'Unione europea un'altra svolta garantista*, cit., 7, il quale osserva che neppure in materia di intercettazioni è previsto un vaglio in concreto circa l'effettiva gravità del reato per cui si procede, potendosi peraltro escludere che il principio di proporzionalità risulti pienamente tutelato dalla più elevata soglia edittale individuata dall'art. 266 co. 1 Cpp (nella misura di 5 anni nel massimo), poiché il pericolo di ingerenze sproporzionate rilevato dalla Corte deriva dalla mancata considerazione di una soglia minima edittale.

anzitutto, una valutazione di proporzionalità in astratto, nell'ambito della quale, peraltro, le istanze connesse all'accertamento dei reati e alla salvaguardia della sicurezza non dovrebbero certo essere trascurate. Infatti, la limitazione delle prerogative individuali conseguente al trasferimento dei dati ben potrebbe risultare proporzionata in relazione all'esigenza di perseguire reati di una certa gravità.

Oltre al prospettato bilanciamento legislativo, la norma dovrebbe essere strutturata in modo da consentire un vaglio avente ad oggetto la gravità in concreto del reato in relazione all'ingerenza conseguente al trasferimento dei dati, che oggi pare ineludibile alla luce della citata sentenza della Grande Sezione. Infatti, se è vero che una simile valutazione del giudice si impone in occasione della prima acquisizione dei dati, sembra doveroso che lo stesso vaglio debba essere compiuto anche in relazione al diverso reato per il quale si procede nella sede presso la quale si vogliono trasferire le suddette informazioni.

Occorre dunque un calibrato intervento del legislatore: come si è visto, gli interessi prioritari in concorso tra loro sono infatti molteplici, oltre che in continua evoluzione. Una nuova disciplina sulla circolazione dei dati, magari inserita nel contesto di una riforma organica della *data retention*, dovrebbe avere particolare riguardo alle nuove esigenze di tutela dei diritti fondamentali che si impongono dinanzi allo sviluppo tecnologico.

È soprattutto il diritto alla riservatezza, ormai ampiamente valorizzato sul piano sovranazionale e internazionale, a esigere una più adeguata considerazione da parte del legislatore interno anche nella materia processuale penale. Da tempo la dottrina ammonisce circa l'urgenza di una tutela degli individui nella dimensione digitale, secondo una concezione che affianchi alle classiche garanzie afferenti alla libertà personale una protezione del «corpo elettronico»[95].

[95] Questo l'insegnamento di S. Rodotà, Privacy, *libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, in *www.privacy.it*, nello stesso senso, Id., *Comunicato Stampa del Garante per la protezione dei dati personali*, in *www.privacy.it*, 16.9.2004, in cui si sottolinea l'importanza dell'*habeas data*, «ossia di una protezione integrale della persona nella dimensione elettronica che adempie la stessa funzione di garanzia delle libertà che ha storicamente svolto l'*habeas corpus*: l'impegno a rispettare il corpo e la libertà»; per G. Alpa, *L'intelligenza artificiale*, cit., 85, «il dato personale, proprio perché legato alla persona, ne compone l'"identità digitale', quasi fosse una proiezione della persona stessa, "una sua parte"». Sul tema, v. L. Lupária, *Privacy, diritti della persona e processo penale*, cit., 1464, secondo il quale occorre interrogarsi «sui riflessi connessi alle garanzie processuali di una nuova concezione «integrale» della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che, ormai, è al contempo "fisico" ed "elettronico"»; nello stesso senso M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., 58. In tema di *habeas data*, v. anche B. Galgani, *Giudizio penale,* habeas data *e garanzie fondamentali*, in *www.archiviopenale.it*, 2019, 1.

Di tali aspetti il legislatore dovrebbe tenere conto nell'ambito dell'auspicato "cantiere" sulla prova tecnologica e sulla tutela dei diritti fondamentali nel processo penale[96].

[96] Per M. Gialuz, *Premessa*, in *Diritto di Internet*, supplemento al fascicolo 3/2020, cit., urge «aprire un ambizioso cantiere dedicato alla prova tecnologica e ai diritti fondamentali nel processo penale»; sul tema v. anche R. Orlandi, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *RIDPP* 2014, 1154, secondo il quale sarebbe auspicabile «che pure la legge italiana adeguasse la lista dei diritti fondamentali all'evoluzione tecnologica, così da trarne le dovute conseguenze sul piano della disciplina processuale».